UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,499	05/10/2001	Walter E. Tuvell	G0008/7005	6408

21127 7590 11/02/2004

KUDIRKA & JOBSE, LLP
ONE STATE STREET
SUITE 800
BOSTON, MA 02109

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/852,499	TUVELL, WALTER E.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 5, 10, 15, 20, 25, 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claims 5, 10, 15, 20, 25, 30 recite the limitation "the mask generation function" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-2, 4, 6-7, 9, 26-27, 29, 32 rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art (admission) in view of Viavant et al (U.S. 5,784,566).

As per claims 1, 6, 26, 32, admission discloses a counter mode block cipher that breaks a message into text bytes and encrypts each text byte with a fixed, secret key with a keysize, generating a random byte sequence for each message and conveying a key to the block cipher so that each text byte is encrypted with the key (see pages 2-3 where the random byte sequence is the initialization vector).

Admission fails to disclose generating a random byte sequence for each message and combining the random byte sequence with the key to form a modified key.

However, Viavant et al discloses combining the random byte sequence with the key to form a modified key (see column 11 lines 25-35).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Viavant et al's method for creating a modified key in admission's ciphering system.

Motivation to do so would have been to create a new key (see Viavant et al column 11 lines 25-35).

As per claims 2, 7, 27, the modified admission and Viavant et al system discloses the random byte sequence has same size as the keysize and step comprises combining the random byte sequence with the key with a bitwise exclusive-OR function (see Viavant et al column 11 lines 25-35).

As per claims 4, 9, 29, the modified admission and Viavant et al system discloses the random byte sequence is non-secret (see admission page 2 paragraph 10).

7. Claims 3, 5, 8, 10, 28, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified admission and Viavant et al system as applied to claims 1, 6, 26 above, and further in view of Kaliski (Security Dynamics).

As per claims 3, 5, 8, 10, 28, 30, the modified admission and Viavant et al system fails to disclose concatenating the random byte sequence to the key and passing it through a one-way mask generation function.

However, Kaliski discloses such a concatenation (see pages 8-9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Kaliski's method for generating a new key through concatenation and a one-way mask generation function in the modified admission and Viavant et al's ciphering system.

Motivation to do so would have been to derive many keys from a password and a salt (Kaliski see page 8).

8. Claims 11-12, 14, 16-17, 19, 21-22, 24, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified admission and Viavant et al and further in view of Krishnan et al (6,141,968).

As per claims 11, 16, 21, 31, the modified admission and Viavant et al system discloses a stream cipher that encrypts a continuous byte stream of messages with a fixed, secret key with a keysize (see admission page 4) combining the random byte sequence with the key to form a modified key (see column 11 lines 25-35) and conveying the modified key to the stream cipher and each message is encrypted with the modified key (see admission page 4).

The modified admission and Viavant et al fails to disclose generating a random byte sequence for each message.

However, Krishnan et al discloses generating a random byte sequence for each message (see column 3 lines 1-6 where a key is a random sequence of bytes).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Krishnan et al's method for generating random byte sequences for each message in the modified admission and Viavant et al's ciphering system.

Motivation to do so would have been to ensure the entire unencrypted message is never visible at any one time (see Krishnan et al column 3 lines 1-6).

As per claims 12, 17, 22, the modified admission Viavant et al and Krishnan et al system discloses the random byte sequence has same size as the keysize and step comprises combining the random byte sequence with the key with a bitwise exclusive-OR function (see Viavant et al column 11 lines 25-35).

As per claims 14, 19, 24, the modified admission Viavant et al and Krishnan et al system discloses the random byte sequence is non-secret (see Viavant et al column 11 lines 25-35).

9. Claims 13, 15, 18, 20, 23, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified admission, Viavant et al and Krishnan et al system as applied to claims 11, 16, 21 above, and further in view of Kaliski (Security Dynamics).

As per claims 13, 15, 18, 20, 23, 35, the modified admission, Viavant et al and Krishnan et al system fails to disclose concatenating the random byte sequence to the key and passing it through a one-way mask generation function.

However, Kaliski discloses such a concatenation (see pages 8-9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Kaliski's method for generating a new key through concatenation and a one-way mask generation function in the modified admission, Viavant et al and Krishnan et al's ciphering system.

Motivation to do so would have been to derive many keys from a password and a salt (Kaliski see page 8).

10. Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuchuta (EP 0422230A) and further in view of Schneier (Applied Cryptography).

As per claims 1-32, are rejected as in the international search report for PCT/US01/15318). The applicants are requested to provide copies, if any, of the written opinion and/or preliminary international examination report of the corresponding PCT application.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

MJP